doi:10.1631/FITEE.1800523

题目：基于基因视角的恶意代码同源性判定

概要：恶意代码同源性判定对攻击事件溯源、应急响应方案处置以及事件发展趋势预测有重要作用。目前，恶意代码同源性判定以人工分析为主，效率较低，对安全事件的爆发无法快速响应。因此，提出一种新的从基因视角分析的恶意代码同源性判定方法。恶意代码基因由表示家族同源性的子图组成。通过筛选关键应用程序接口和利用社团划分算法，从函数依赖图中提取关键子图作为恶意代码基因。然后，设计一种频繁子图挖掘算法发现恶意代码家族的共有基因，并对基因编码。最后，利用家族共有基因指导恶意代码同源性判定。对公开数据集的分类和实验结果表明，分类准确率达97%，且效率较高。

关键词：恶意代码分类；基因视角；函数依赖图；同源性分析